UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/780,622	02/19/2004	Kia Silverbrook	ZE029US	2762

24011 7590 02/17/2006

SILVERBROOK RESEARCH PTY LTD
393 DARLING STREET
BALMAIN, NSW 2041
AUSTRALIA

EXAMINER	
LIPMAN, JACOB	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 02/17/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/780,622	SILVERBROOK, KIA	
	Examiner	Art Unit	
	Jacob Lipman	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Priority

1. Applicant's claim for the benefit of a prior-filed application under 35 U.S.C. 119(e) or under 35 U.S.C. 120, 121, or 365(c) is acknowledged. Applicant has not complied with one or more conditions for receiving the benefit of an earlier filing date under 35 U.S.C. [1] as follows:

The later-filed application must be an application for a patent for an invention that is also disclosed in the prior application (the parent or original nonprovisional application or provisional application). The disclosure of the invention in the parent application and in the later-filed application must be sufficient to comply with the requirements of the first paragraph of 35 U.S.C. 112. See *Transco Products, Inc. v. Performance Contracting, Inc.*, 38 F.3d 551, 32 USPQ2d 1077 (Fed. Cir. 1994).

The disclosure of the prior-filed application, Application No. 09/516,874, fails to provide adequate support or enablement in the manner provided by the first paragraph of 35 U.S.C. 112 for one or more claims of this application. A couple of examples of unsupported materials are that the examiner found no reference to integrated circuits or accessories in the disclosure of 09/516,874.

Specification

2. The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

3. The specification should also be amended to include the patent number of the application it claims benefit of.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claim 3 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 3 recites the limitation "advance R to next in sequence" in line 22. There is insufficient antecedent basis for this sequence in the claim.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1-3 and 5, as best understood, are rejected under 35 U.S.C. 102(b), or 35 U.S.C. 102(e) if applicant can support the claim of priority, has being anticipated by Doljack, USPN 6,442,276.

With regard to claims 1 and 5, Doljack discloses a method of authenticating memory space of an authorized accessory of a device (column 1 lines 5-12), the method including the steps of: storing secret key, K1 (public/private keys) and K2 (hash function), in an integrated circuit of the device (column 4 lines 35-56) and in the memory space of the accessory (column 4 lines 57-62), generating a random number R (column 5 lines 55-60) and a first parameter being a function of R using the key K1 (public/private key) of the integrated circuit of the device (column 11 lines 9-15), calling a read function defined by the accessory using a second parameter being a function of R using the key K1 of the accessory (column 11 lines 15-19), and if the first and second parameters are equivalent (if the second parameter decrypts), calling a test function of the integrated circuit using a fourth parameter being a function of R using the key K2 of the integrated circuit device (column 11 lines 19-22), and returning a one if the third and fourth parameters are equivalent (column 11 lines 22-23).

With regard to claim 2, Doljack discloses the test and read functions are one-way hashes (column 11 lines 19-23).

With regard to claim 3, Doljack discloses advancing the random number to next in sequence when generating (column 2 lines 54-61).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claim 4, as best understood, is rejected under 35 U.S.C. 103(a) as being unpatentable over Doljack.

With regard to claim 4, Doljack discloses the apparatus of claim 3, as disclosed above, including using a random number generator. Doljack does not specify any specific random number generator to use. The examiner takes official notice that using an LSFR is a common way to generate random numbers, especially ones that don't repeat, a stated motivation in Doljack (column 2 lines 54-61). Support for this official notice can be found in numerous references, including Gilham, USPN 4,757,532 (column 6 lines 1-5). It would have been obvious for one of ordinary skill in the art to use an LFSR in Doljack to generate random numbers.

10. Claims 1-5, as best understood, are further rejected under 35 U.S.C. 103(a) as being unpatentable over Ford et al. in Secure Electronic Commerce.

With regard to claims 1-3 and 5, Ford discloses a challenge response system in which a host sends a random number to an claimant (page 129 section b) and the claimant responds by hashing the number with a hash function (key). Ford does not disclose the host and claimant having duplicate keys, and performing the authentication twice. In re Harza, 274 F.2d 669, 671, 124 USPQ 378, 380 (CCPA 1950) shows that duplicating a part for a multiple effect would be obvious to one of ordinary skill in the art. The examiner further takes official notice that making the claimant responsible for two keys would help prevent birthday attacks on the host. It would have been obvious for one of ordinary skill in the art to perform the method of Ford twice to increase security.

With regard to claim 4, Ford discloses the apparatus of claim 3, as disclosed above, including using a random number generator. Ford does not specify any specific random number generator to use. The examiner takes official notice that using an LSFR is a common way to generate random numbers, especially ones that don't repeat, a stated motivation in Ford (page 129 section b lines 6-8). Support for this official notice can be found in numerous references, including Gilham, USPN 4,757,532 (column 6 lines 1-5). It would have been obvious for one of ordinary skill in the art to use an LFSR in Ford to generate random numbers.

11. Claims 1-5, as best understood, are rejected under 35 U.S.C. 103(a), as being unpatentable over Schneier, USPN 6,099,408.

With regard to claims 1-3 and 5, Schneier discloses a method of authenticating memory space of an authorized accessory of a device (column 1 lines 55-64), the method including the steps of: storing secret key, K1 (hash function), in an integrated circuit of the device (column 11 lines 22-24) and in the memory space of the accessory (column 11 lines18-21), generating a random number R (column 11 lines 18-21) and a first parameter being a function of R using the key K1 (hashing R) of the integrated circuit of the device (column 11 lines 18-21), calling a read function defined by the accessory using a second parameter being a function of R using the key K1 of the accessory (column 11 lines 22-24), and if the first and second parameters are equivalent returning a one if the third and fourth parameters are equivalent (column 11 lines 24-26). Schneier does not disclose the host and claimant having duplicate keys, and performing the authentication twice. In re Harza, 274 F.2d 669, 671, 124 USPQ

378, 380 (CCPA 1950) shows that duplicating a part for a multiple effect would be obvious to one of ordinary skill in the art. The examiner further takes official notice that making the claimant responsible for two keys would help prevent birthday attacks on the host. It would have been obvious for one of ordinary skill in the art to perform the method of Schneier twice to increase security.

With regard to claim 4, Schneier discloses the apparatus of claim 3, as disclosed above, including using a random number generator. Schneier does not specify any specific random number generator to use. The examiner takes official notice that using an LSFR is a common way to generate random numbers, especially ones that don't repeat, a stated motivation in Ford (page 129 section b lines 6-8). Support for this official notice can be found in numerous references, including Gilham, USPN 4,757,532 (column 6 lines 1-5). It would have been obvious for one of ordinary skill in the art to use an LFSR in Schneier to generate random numbers.

Conclusion

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jacob Lipman whose telephone number is 571-272-3837. The examiner can normally be reached on M-Th 7 AM-3 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on 571-272-3838. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

JL

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100